In the Specification

Please replace the paragraph beginning at page 1, line 6, with the following rewritten paragraph:

-- U. S. patent application Serial ~~No. 09/_____, assignee docket number END9-2000-0092-US1~~ No. 09/813,911, entitled "SYSTEM AND METHOD FOR NESTING VIRTUAL PRIVATE NETWORKING CONNECTIONS WITH COINCIDENT ENDPOINTS", filed concurrently herewith, and U. S. patent application Serial No. 09/240,720 filed 29 Jan 1999 by Edward B. Boden and Franklin A. Gruber for "SYSTEM AND METHOD FOR NETWORK ADDRESS TRANSLATION INTEGRATION WITH IP SECURITY", now U. S. Patent No. 6,615,357, issued 2 Sep 2003, are assigned to the same assignee hereof and contain subject matter related, in certain respect, to the subject matter of the present application. The above-identified patent applications are incorporated herein by reference.--.

Please replace the paragraph beginning at page 3, line 1, with the following rewritten paragraph:

-- A typical configuration for doing this connection

of PC 10 to a server within internal network 18 uses two VPN connections (also referred to as tunnels) t1 20 and t2 22. ~~connection~~ Connection t1 20 begins at ISP 12 and ends at gateway 16.--.

Please replace the paragraph beginning at page 4, line 8, with the following rewritten paragraph:

-- Network address translation (NAT) is a widely-deployed approach by which an enterprise can support remote users while avoiding address collisions within its own internal network. However, NAT is incompatible with VPN for architectural reasons. U. S. patent application Serial No. 09/240,720, now U. S. Patent No. 6,615,357, issued 2 Sep 2003, and other applications therein referenced, provide a solution that integrates NAT with VPN.--.

Please replace the paragraph beginning at page 8, line 11, with the following rewritten paragraph:

-- Figure 4 illustrates VPN NAT, type c: IDci translated for responder-mode conversations (also known as 'source-in' VPN NAT). This Figure 4 corresponds to

Figure 6 of U.S. patent application S/N 09/240,720, filed 29 Jan 1999, now U. S. Patent No. 6,615,357, issued 2 Sep 2003.--.

Please replace the paragraph beginning at page 9, line 6, with the following rewritten paragraph:

-- In copending U.S. Patent application, S/N 09/813,911, filed concurrently herewith ~~assignee docket END9 2000 0092 US1~~, Figure 2, scenario C illustrates the solution to definition of client IP addresses by using a third encapsulation on the L2TP connection to assign routable IP address known to the enterprise (represented by enterprise gateway 16.) Referring to Figure 2 in the present application, another solution, based on VPN NAT, is illustrated which has the advantage of not requiring a third encapsulation. Together, these form a full solution for a remote VPN user 10.--.

Please replace the paragraph beginning at page 13, line 12, with the following rewritten paragraph:

-- In step 110, inner connection 54 is started. In

the scenarios which apply to the present invention, inner connections t2 54 are initiated by client 10. More specifically, the inner connection t2 for both this application and for copending application S/N 09/813,911, filed concurrently herewith ~~EN9-2000-0092 US1~~ are initiated remotely (with respect to the gateway 50).---.

Please replace the paragraph beginning at page 13, line 18, with the following rewritten paragraph:

-- In step 112, ~~or outbound~~ for outbound SA, gateway propagates VPN NAT rule from outer tunnel t1 52 to inner tunnel t2 54, when the inner tunnel t2 is started.--.

Please replace the paragraph beginning at page 15, line 8, with the following rewritten paragraph:

-- Referring further to Figure 2, traffic flow for outbound traffic from network 18 at point A is to local coincident endpoint 56 ~~point A1 on~~ point A1 or for encapsulation on inner connection t2 54; it is here NAT occurs on packets before IPsec is applied, then

encapsulated in the inner t2 54 tunnel. From point A1, the packet is logically encapsulated in outer connection at point B1, decapsulated at ISP 12 point C1, flows to inner connection t2 54 and is finally decapsulated at client 10. Traffic flowing from client 10 to network 18 follows the reverse path, with decapuslation and encapsulation also reversed. Encapsulation involves adding headers to a packet, and decapsulation removes those headers.---.

Please replace the paragraph beginning at page 16, line 1, with the following rewritten paragraph:

-- Referring to Figure 4, VPN NAT source-in executes to translate IDci for responder-mode conversations as follows: in step <-2>, for remotely initiated conversations, at start, since NAT is requested, implicit MAP rule 158 <MAP ihs TO rhs> is created, copying responder mode NAT flag IDci 152 to rhs 154. In step <-1>, the ip address is obtained from the appropriate pool 150 (associated with IDir) and copied to lhs 156. In step <0>, after IKE negotiation is complete using rhs 154, implicit rule 160 is loaded. When processing inbound packets, if in step <1> src ip

172 matches rhs 168, in step <2> source ip 172 is translated to lhs 166. When processing outbound datagrams, if in step <3> destination 164 matches lhs 166, in step <4> destination ip 164 is translated to rhs 168. (Note that the inbound destination IP address 170 and the outbound source IP address 162 are not changed.)--.